Ref. 1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－285156

(43)公開日　平成10年(1998)10月23日

| (51)Int.Cl.[6] | 識別記号 | ＦＩ | |
|---|---|---|---|
| Ｈ０４Ｌ　9/32 | | Ｈ０４Ｌ　9/00 | ６７５Ｂ |
| 9/08 | | | ６０１Ｆ |
| | | | ６７５Ｄ |

審査請求　未請求　請求項の数４　ＯＬ　（全 11 頁）

(21)出願番号　特願平9－92436

(22)出願日　平成９年(1997)４月10日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(71)出願人　000102717
エヌ・ティ・ティ・ソフトウェア株式会社
神奈川県横浜市中区山下町223番１

(72)発明者　橋本　正一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　村田　祐一
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　三好　秀和　（外１名）

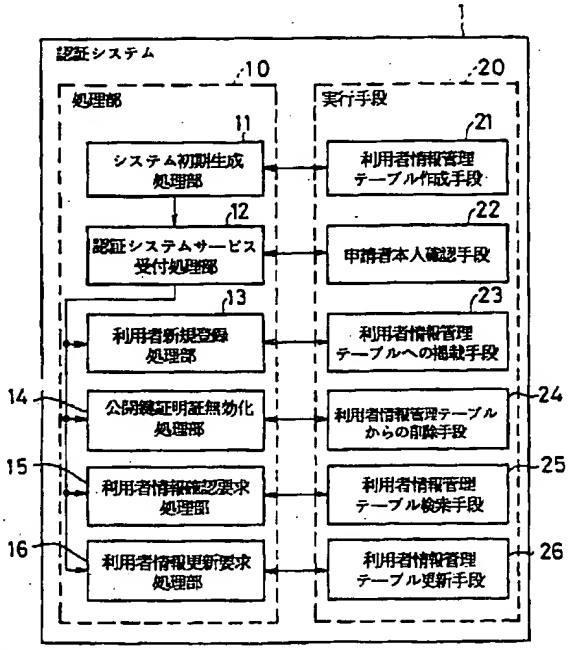
最終頁に続く

(54)【発明の名称】　認証システムにおける利用者情報管理装置

(57)【要約】

【課題】　本発明は、利用者情報を確実に管理することを可能とする認証システムにおける利用者情報管理装置を提供することを目的とする。

【解決手段】　公開鍵暗号方式を用いた認証システムにおける利用者情報管理装置であって、利用者情報が当該利用者名により管理される利用者情報管理テーブル２１ａと、この利用者情報管理テーブル２１ａへの掲載要求、新規登録、公開鍵証明証の無効化、利用者情報確認或いは更新の申請があった場合、この申請の利用者名が申請者本人であるか否かを確認する申請者本人確認手段２２で利用者名が申請者本人であることが確認されたときに、前記利用者情報管理テーブルに当該利用者情報を利用者毎に新規登録の掲載、公開鍵証明証の無効化、利用者情報確認或いは更新等を行う手段を備える。



1

【特許請求の範囲】

【請求項１】　特定される公開鍵の持ち主であることを証明する公開鍵証明証を当該持ち主に係る情報である利用者情報と共に管理する公開鍵暗号方式を用いた認証システムにおける利用者情報管理装置であって、

前記利用者情報が当該利用者名により管理される利用者情報管理テーブルと、

この利用者情報管理テーブルへの掲載要求の申請があったときにはこの申請の利用者名が申請者本人であるか否かを確認する申請者本人確認手段と、

この申請者本人確認手段で前記利用者名が申請者本人であることが確認されたときに、前記利用者情報管理テーブルに当該利用者情報を利用者毎に掲載する掲載手段とを有することを特徴とする認証システムにおける利用者情報管理装置。

【請求項２】　特定される公開鍵の持ち主であることを証明する公開鍵証明証を当該持ち主に係る情報である利用者情報と共に管理する公開鍵暗号方式を用いた認証システムにおける利用者情報管理装置であって、

前記利用者情報が当該持ち主の利用者名により管理される利用者情報管理テーブルと、

この利用者情報管理テーブルの利用に際し申請された利用者名が申請者本人であるか否かを確認する申請者本人確認手段と、

この申請者本人確認手段で前記利用者名が申請者本人であることが確認され、前記申請が利用者情報管理テーブルからの当該持ち主に係る利用者情報の削除であるときには当該利用者情報を利用者情報管理テーブルから削除する削除手段とを有することを特徴とする認証システムにおける利用者情報管理装置。

【請求項３】　特定される公開鍵の持ち主であることを証明する公開鍵証明証を当該持ち主に係る情報である利用者情報と共に管理する公開鍵暗号方式を用いた認証システムにおける利用者情報管理装置であって、

前記利用者情報が当該持ち主の利用者名により管理される利用者情報管理テーブルと、

この利用者情報管理テーブルの利用に際し申請された利用者名が申請者本人であるか否かを確認する申請者本人確認手段と、

この申請者本人確認手段で前記利用者名が申請者本人であることが確認され、前記申請が利用者情報管理テーブルからの利用者情報の読み出しであるときには当該情報管理テーブルを検索し該当利用者情報を読み出す利用者情報管理テーブル検索手段とを有することを特徴とする認証システムにおける利用者情報管理装置。

【請求項４】　特定される公開鍵の持ち主であることを証明する公開鍵証明証を当該持ち主に係る情報である利用者情報と共に管理する公開鍵暗号方式を用いた認証システムにおける利用者情報管理装置であって、

前記利用者情報が当該持ち主の利用者名により管理される利用者情報管理テーブルと、

2

この利用者情報管理テーブルの利用に際し申請された利用者名が申請者本人であるか否かを確認する申請者本人確認手段と、

この申請者本人確認手段で前記利用者名が申請者本人であることが確認され、前記申請が利用者情報管理テーブルに掲載される利用者情報の更新であるときには当該情報管理テーブルの該当利用者情報を申請された利用者情報に更新する利用者情報管理テーブル更新手段とを有することを特徴とする認証システムにおける利用者情報管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、公開鍵暗号方式で利用される公開鍵の正当性を証明する認証システムにおける利用者情報管理装置に関するものである。

【０００２】

【従来の技術】コンピュータネットワーク上で電子データ交換（ＥＤＩ：Electronic Data Interchange）や電子商取引（ＥＣ：Electronic Commerce）を実現する際には、盗聴／なりすまし／改ざん／送信否認などの脅威が想定される。そのため、これら脅威からシステムを防御するために、一般的に暗号通信やディジタル署名通信が用いられる。この暗号方式は、例えば参考文献「Diffie,W.and Helman,M.：New Directions in Cryptography,IEEE Trans.Inf.Theory,IT-22,6 pp.644-654,1976」で発表されており、世の中で広く知られるところとなっている。

【０００３】このような公開鍵暗号方式では、一般に広く公開しておく公開鍵と、自分のみが知り得る秘密鍵の２種類の鍵を用いて通信が行われる。ここで、公開鍵を単に周知するだけでは他人を装って周知する「なりすまし」と呼ばれる脅威が考えられることから、公開鍵の正当な持ち主であることを証明する第三者機関が必要であり、それが認証局（ＣＡ：Certification Authority)と呼ばれるものである。

【０００４】この認証局を含む認証システムは、コンピュータネットワーク上で取引関係にある企業間での取引を電子交換する電子データ交換やコンピュータネットワーク上で情報を伝達、処理し電子決済等の商取引を行う電子商取引を実現する際に、送信データの秘匿性や改ざん防止の目的で利用される公開鍵暗号方式に関して、その公開鍵証明証を発行／管理するシステムである。すなわち、認証システムは、日本の実社会で、実印の持ち主を証明する印鑑証明書を役所が発行するのと同様に、ディジタル通信の世界で、公開鍵の持ち主を証明する公開鍵証明証を発行する機能を持ったシステムであるということができる。

【０００５】一般的に認証システムの機能として、次の４つが知られている。

（1）公開鍵登録機能…利用者が申請した公開鍵に対して、公開鍵証明証を作成／登録／発行する。
（2）証明証参照機能…認証システムで管理している公開鍵証明証を利用者から参照可能とする。
（3）公開鍵無効化機能…公開鍵証明証を無効化し、無効化リストに掲載する。
（4）無効化リスト参照機能…無効化された公開鍵証明証の一覧を利用者から参照可能とする。

【0006】これらの機能は、コンピュータシステムや暗号アルゴリズムにより既に提供されている一般的な手段を用いて構築可能であり、申請時に申請書を用いた依頼を行うこと、認証システムと利用者の間ではディジタル署名通信を行うこと、公開鍵証明証や無効化リストをディレクトリやデータベースに管理しておくこと、などの基本的な構成方式についても、既に一般的方法であると認知されている。

【0007】さて、認証システムは、利用者が提示する申請書から必要な情報を抜き出して、公開鍵証明証を作成することになる。ところが、この利用者から提示された申請書には、通常、公開鍵証明証の作成に必要な情報以外にも、認証システムの運営に必要な情報である、認証システムが利用者との連絡を取るための情報や、課金を行うための口座情報などの記載が求められている。そのため、これらの公開鍵証明証に載せない利用者個人の情報である利用者情報は、通常、外部に漏れないように、認証システムの内部において公開鍵証明証とは別管理にされている。また、認証システムの運営者が、これら利用者情報を利用して当該利用者の個人情報を参照する際には、当該運営者が利用者名などを検索キーとして個々にシステム内を検索するようにしていた。

【0008】

【発明が解決しようとする課題】しかしながら、通常、利用者が認証システムに対して申請する情報の中で、公開鍵証明証に載せない利用者情報は、世の中に公開される公開鍵証明証とは別に、認証システムの内部に閉じて管理されているため、利用者が、自分の利用者情報に対する確認や更新といった操作を、認証システムの運営者を介すこと無く行うことは困難である。

【0009】例えば、認証システムから利用者に対する連絡の通知方法について、利用者が当該利用者への通知を電子メールを利用して行うことを希望して、その旨を個人情報として申請している場合についてみると、何らかの理由により利用者のシステムが停止した場合には、利用者は郵便による通知に変更することを申請しなければならない。このような場合、利用者は、これら認証システムで管理されている利用者情報に直接アクセスして、掲載内容を確認し、更新処理を行うことはできない。そのため、利用者は認証システムに問い合わせてオペレータに現状を確認してもらい、その後に変更依頼を申請するといった手間がかかり、認証システムの利用者情報に対する管理に負荷がかかることになる。

【0010】また、例えば利用者によって当該公開鍵証明証を無効化する公開鍵証明証の無効化申請が行われ、利用者の公開鍵証明証が認証システム内に無くなった場合、その利用者の個人情報も管理する必要が無くなることになるが、利用者情報は公開鍵証明証とは別管理されているため、その利用者の利用者情報が残されたままとなる。そのため、利用者情報を管理する記憶領域に無駄が生じる可能性があるなど、利用者情報が確実に管理されないといった問題が生じる場合もある。

【0011】本発明は、上記課題に鑑みてなされたもので、認証システムの運営において必要な利用者情報に対して、利用者が、自分の情報に対してのみ、直接アクセスして確認、更新することを可能とし、また認証システムは、公開鍵証明証の管理と関連付けて、利用者情報の登録や削除処理を行い、利用者情報を確実に管理することを可能にする認証システムにおける利用者情報管理装置を提供することを目的とする。

【0012】

【課題を解決するための手段】前述した目的を達成するために、本発明のうちで請求項1記載の発明は、特定される公開鍵の持ち主であることを証明する公開鍵証明証を当該持ち主に係る情報である利用者情報と共に管理する公開鍵暗号方式を用いた認証システムにおける利用者情報管理装置であって、前記利用者情報が当該利用者名により管理される利用者情報管理テーブルと、この利用者情報管理テーブルへの掲載要求の申請があったときにはこの申請の利用者名が申請者本人であるか否かを確認する申請者本人確認手段と、この申請者本人確認手段で前記利用者名が申請者本人であることが確認されたときに、前記利用者情報管理テーブルに当該利用者情報を利用者毎に掲載する掲載手段とを有することを要旨とする。

【0013】請求項1記載の本発明では、公開鍵証明証に載せない利用者の個人情報を、公開鍵証明証と同様に利用者名をキーにして認証システムが管理し、利用者から本人の利用者情報に対して利用者情報管理テーブルへの掲載要求があった際には、申請書に付いた電子署名を検証して、申請者の本人確認を自動的に行った後に、利用者情報に対する操作を許可し、利用者からの公開鍵証明証の新規登録等の掲載の申請に対し、これらの処理の一部として、必要に応じて掲載手段が利用者情報の登録を行うことを可能とする。

【0014】本発明のうちで請求項2記載の発明は、特定される公開鍵の持ち主であることを証明する公開鍵証明証を当該持ち主に係る情報である利用者情報と共に管理する公開鍵暗号方式を用いた認証システムにおける利用者情報管理装置であって、前記利用者情報が当該持ち主の利用者名により管理される利用者情報管理テーブルと、この利用者情報管理テーブルの利用に際し申請され

た利用者名が申請者本人であるか否かを確認する申請者本人確認手段と、この申請者本人確認手段で前記利用者名が申請者本人であることが確認され、前記申請が利用者情報管理テーブルからの当該持ち主に係る利用者情報の削除であるときには当該利用者情報を利用者情報管理テーブルから削除する削除手段とを有することを要旨とする。

【００１５】請求項２記載の本発明では、公開鍵証明証に載せない利用者の個人情報を、公開鍵証明証と同様に利用者名をキーにして認証システムが管理し、利用者から本人の利用者情報に対して利用者情報管理テーブルからの削除要求があった際には、申請書に付いた電子署名を検証して、申請者の本人確認を自動的に行った後に、利用者情報に対する操作を許可し、これらの処理の一部として、削除手段が利用者情報の削除を行うことを可能とする。

【００１６】本発明のうちで請求項３記載の発明は、特定される公開鍵の持ち主であることを証明する公開鍵証明証を当該持ち主に係る情報である利用者情報と共に管理する公開鍵暗号方式を用いた認証システムにおける利用者情報管理装置であって、前記利用者情報が当該持ち主の利用者名により管理される利用者情報管理テーブルと、この利用者情報管理テーブルの利用に際し申請された利用者名が申請者本人であるか否かを確認する申請者本人確認手段と、この申請者本人確認手段で前記利用者名が申請者本人であることが確認され、前記申請が利用者情報管理テーブルからの利用者情報の読み出しであるときには当該情報管理テーブルを検索し該当利用者情報を読み出す利用者情報管理テーブル検索手段とを有することを要旨とする。

【００１７】請求項３記載の本発明では、公開鍵証明証に載せない利用者の個人情報を、公開鍵証明証と同様に利用者名をキーにして認証システムが管理し、利用者から本人の利用者情報に対して利用者情報管理テーブルから本人の利用者情報の読み出し要求があった際には、申請書に付いた電子署名を検証して、申請者の本人確認を自動的に行った後に、利用者情報に対する操作を許可し、これらの処理の一部として、利用者情報管理テーブル検索手段が利用者情報管理テーブルを検索し利用者情報の読み出しを行うことを可能とする。

【００１８】本発明のうちで請求項４記載の発明は、特定される公開鍵の持ち主であることを証明する公開鍵証明証を当該持ち主に係る情報である利用者情報と共に管理する公開鍵暗号方式を用いた認証システムにおける利用者情報管理装置であって、前記利用者情報が当該持ち主の利用者名により管理される利用者情報管理テーブルと、この利用者情報管理テーブルの利用に際し申請された利用者名が申請者本人であるか否かを確認する申請者本人確認手段と、この申請者本人確認手段で前記利用者名が申請者本人であることが確認され、前記申請が利用者情報管理テーブルに掲載される利用者情報の更新であるときには当該情報管理テーブルの該当利用者情報を申請された利用者情報に更新する利用者情報管理テーブル更新手段とを有することを要旨とする。

【００１９】請求項４記載の本発明では、公開鍵証明証に載せない利用者の個人情報を、公開鍵証明証と同様に利用者名をキーにして認証システムが管理し、利用者から本人の利用者情報に対して利用者情報の変更、追加、訂正等の更新要求があった際には、申請書に付いた電子署名を検証して、申請者の本人確認を自動的に行った後に、利用者情報に対する操作を許可し、これらの処理の一部として、利用者情報管理テーブル更新手段が利用者情報の更新を行うことを可能とする。

【００２０】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図１は本発明の一実施の形態に係る認証システムの構成を示すブロック図である。図１において、認証システム１は処理部１０とこの処理部１０に対応して設けられる実行手段２０によって構成される。処理部１０は、システム初期生成処理部１１、認証システムサービス受付処理部１２、利用者新規登録処理部１３、公開鍵証明証無効化処理部１４、利用者情報確認要求処理部１５及び利用者情報更新要求処理部１６によって構成される。

【００２１】また、システム初期生成処理部１１に対応して利用者情報管理テーブル作成手段２１、認証システムサービス受付処理部１２に対応して申請者本人確認手段２２、利用者新規登録処理部１３に対応して利用者情報管理テーブルへの掲載手段２３、公開鍵証明証無効化処理部１４に対応して利用者情報管理テーブルからの削除手段２４、利用者情報確認要求処理部１５に対応して利用者情報管理テーブル検索手段２５、利用者情報更新要求処理部１６に対応して利用者情報管理テーブル更新手段２６が設けられている。

【００２２】以下、各処理部における実行手段の作用を処理手順に従って説明する。まず、ステップＳ１で、システム初期生成処理部１１において、利用者情報管理テーブル作成手段２１を用いて、図２に示すような利用者名をキーとする利用者情報管理テーブル２１ａを設ける。

【００２３】続く、ステップＳ２では、認証システムサービス受付処理部１２において、申請者本人確認手段２２を用いて、受信した申請書２２ａに記載されている申請者名に偽りがないかを、申請書２２ａに付与されている電子署名を検証することによって本人性の確認を行う。

【００２４】次に、申請者が認証システムに対して依頼したサービスが新規登録サービスであった場合、ステップＳ３に進み、利用者新規登録処理部１３において、利用者情報管理テーブル２１ａへの掲載手段２３を用い

て、申請書２２ａから利用者名と利用者情報を読み出し、これを利用者情報管理テーブル２１ａに掲載する。

【００２５】また、申請者が認証システムに対して依頼したサービスが公開鍵証明証無効化サービスであった場合には、ステップＳ４に進み、公開鍵証明証無効化処理部１４において、利用者情報管理テーブル２１ａからの削除手段２４を用いて、申請者の公開鍵証明証が図５に示す公開鍵証明証管理データベース２４ａに残存しないことを確かめてから、利用者情報管理テーブル２１ａにおけるその利用者の項目（利用者名、利用者情報）を削除する。

【００２６】また、申請者が認証システムに対して依頼したサービスが利用者情報の確認サービスであった場合には、ステップＳ５に進み、利用者情報確認要求処理部１５において、利用者情報管理テーブル２１ａの検索手段２５を用いて、該当する利用者情報を取得し、その情報を申請者に送付する。

【００２７】さらに、申請者が認証システムに対して依頼したサービスが利用者情報の更新サービスであった場合には、ステップＳ６に進み、利用者情報更新要求処理部１６において、利用者情報管理テーブル２１ａの更新手段２６を用いて、利用者情報管理テーブル２１ａ内の該当利用者の利用者情報を、申請された利用者情報に置き換えて更新する。

【００２８】次に、本実施形態における処理を各処理部毎に詳細に説明する。まず、図２を参照して、システム初期生成処理部１１におけるシステム初期生成処理について説明する。認証システムのシステム初期生成処理部１１では、各種の初期化処理を行う。その処理の一部として、まず利用者情報管理テーブル作成手段２１を呼び出す。利用者情報管理テーブル作成手段２１では、テーブル記憶領域の確保を行い、この確保された領域に、図２に示すような利用者名と利用者情報の記述欄を持つ利用者情報管理テーブル２１ａを作成する。ここで、テーブル記憶領域はメモリ上、あるいは磁気ディスク等の２次記憶媒体上のどこに存在してもよく、その領域確保は一般のコンピュータシステムが提供している機能によって実現される。

【００２９】次に図３を参照して、認証システムサービス受付処理部１２における認証システムサービス受付処理について説明する。利用者から認証システムに対してサービス依頼の申請が行われると、認証システムでは認証システムサービス受付処理が実施される。その処理の一部として、申請者本人確認手段２２が呼び出される。申請者本人確認手段２２では、申請書２２ａを受信して、申請書２２ａから申請者名を取得し、申請者の公開鍵証明証を公開鍵管理データベースから読み出す。次に申請書２２ａに付与された電子署名を取り出して、これを公開鍵証明証内に含まれる公開鍵を用いて検証し、申請者の本人性、すなわち利用者としての正当性を確認する。

【００３０】尚、申請書２２ａの受信はコンピュータシステムが一般に提供している方法、例えば電子メールなどを用いて実現できる。また、公開鍵証明証管理データベースからの申請者の公開鍵証明証の取得や、申請書２２ａの電子署名の検証は、認証システムで一般的に用意されている公開鍵証明証参照機能や電子署名検証機能を用いることによって実現できる。

【００３１】次に図４を参照して、利用者新規登録処理部１３における利用者新規登録処理について説明する。利用者から受け付けた申請書２２ａに記載された依頼対象サービスが、新規登録サービスの場合、認証システムサービス受付処理部１２におけるサービス振り分け処理によって利用者新規登録処理部１３に処理が移り、そこで利用者情報管理テーブル２１ａへの掲載手段２３が呼び出される。利用者情報管理テーブル２１ａへの掲載手段２３では、申請書２２ａから利用者名と利用者情報を読み出し、これを利用者情報管理テーブル２１ａに利用者名と利用者情報を対応付けて掲載していく。このときの掲載方法については、テーブル記憶領域が確保されている場所に応じて、一般のコンピュータシステムが提供する情報の書き込み機能によって実現できる。

【００３２】次に図５を参照して、公開鍵証明証無効化処理部１４における公開鍵証明証無効化処理について説明する。利用者から受け付けた申請書２２ａに記載された依頼対象サービスが、公開鍵証明証無効化サービスの場合、認証システムサービス受付処理部１２におけるサービス振り分け処理によって、公開鍵証明証無効化処理部１４に処理が移る。公開鍵証明証無効化処理部１４では、利用者が申請した無効化対象の公開鍵証明証を無効化リストに登録し、認証システムが管理する公開鍵証明証管理データベース２４ａからその公開鍵証明証を削除するといった処理が行われる。このとき、この処理の一部として、利用者情報管理テーブル２１ａからの削除手段２４を呼び出す。

【００３３】利用者情報管理テーブル２１ａからの削除手段２４では、まず、申請書２２ａから利用者名を読み出し、その利用者の公開鍵証明証が、認証システムが管理する公開鍵証明証管理データベース２４ａ内にもはや残存しないことを確認する。ここでその利用者の公開鍵証明証が認証システム内に残存していなかった場合、その利用者の利用者情報を認証システムが管理する必要性がなくなることから、利用者情報管理テーブル２１ａから、その利用者の項目（利用者名と利用者情報）を削除する。これによって、利用者情報の管理領域を無駄なく利用することが可能になる。

【００３４】尚、公開鍵証明証データベース２２ｂの検索は、通常の認証システムが保持する機能によって容易に実現可能である。

【００３５】次に図６を参照して、利用者情報確認要求

処理部１５における利用者情報確認要求処理について説明する。利用者から受け付けた申請書２２ａに記載された依頼対象サービスが、利用者情報確認サービスの場合、認証システムサービス受付処理部１２におけるサービス振り分け処理によって利用者情報確認要求処理部１５に処理が移る。利用者情報確認要求処理部１５では、申請者本人の利用者情報に対してのみ確認要求を受け付ける。ここでは、申請者本人確認手段２２において本人確認処理が行われた申請者本人のみの利用者情報に限って確認処理を受け付ける。

【００３６】そこで、利用者情報管理テーブル検索手段２５を呼び出し、本人確認の済んだ申請書内に記載された利用者名を取得し、この利用者名で利用者情報管理テーブル２１ａを検索する。そして、検索した利用者名に該当する利用者情報を読み出し、これを申請者に対して送付することにより、申請者が自分の利用者情報を確認できるようにする。

【００３７】尚、利用者情報の検索は、一般のコンピュータシステムにおいて提供されている情報検索手法を用いることによって容易に実現可能である。

【００３８】次に、図７を参照して、利用者情報更新要求処理部１６における利用者情報更新要求処理について説明する。利用者から受け付けた申請書２２ａに記載された依頼対象サービスが、利用者情報更新サービスの場合、認証システムサービス受付処理部１２におけるサービス振り分け処理によって利用者情報更新要求処理部１６に処理が移る。利用者情報更新要求処理部１６では、申請者本人の利用者情報に対してのみ更新要求を受け付ける。ここでは、申請者本人確認手段２２において本人確認処理が行われた申請者本人のみの利用者情報に限って更新処理を受け付ける。

【００３９】そこで、利用者情報管理テーブル更新手段２６を呼び出し、まず、申請書２２ａから利用者名と、利用者情報の更新情報を取得する。次に利用者情報管理テーブル２１ａにおいて、利用者名を検索し、該当する利用者の利用者情報の欄を、更新情報に置き換えて更新する。

【００４０】尚、利用者情報管理テーブル２１ａにおける利用者情報欄の更新は、一般のコンピュータシステムにおいて提供されている情報の書き込み機能を用いることによって容易に実現可能である。

【００４１】以上の処理により、申請者の利用者情報に対する操作依頼が完了する。上述したように、本実施形態によれば、利用者は、申請書２２ａに電子署名を付けて認証システムに送付することのみによって、自分の利用者情報に限ってその確認や更新の処理を自動的に行うことができ、これによって認証システムが行う利用者情報の管理の手間が軽減される。また、公開鍵証明証の新規登録処理や無効化処理と、利用者情報の登録、削除の処理を関連付けることにより、利用者情報の管理を確実に行うことが可能になる。

【００４２】

【発明の効果】以上説明したように、本発明によって、利用者は、自分の利用者情報に限ってその確認や更新の処理を自動的に行うことが可能になり、これによって認証システムの利用者情報の管理の手間が軽減される。また、公開鍵証明証の登録状況に応じて、利用者情報の登録や削除を行うことが可能になる。したがって、認証システム側は利用者情報の確認サービスや更新サービスを提供でき、また利用者情報の登録処理や削除処理を、公開鍵証明証の管理と関連付けて確実に行うことが可能となる。

【図面の簡単な説明】

【図１】本発明に係る認証システムの構成を示すブロック図である。

【図２】図１におけるシステム初期生成処理を説明するためのブロック図である。

【図３】図１における認証システムサービス受付処理を説明するためのブロック図である。

【図４】図１における利用者新規登録処理を説明するためのブロック図である。

【図５】図１における公開鍵証明証無効化処理を説明するためのブロック図である。

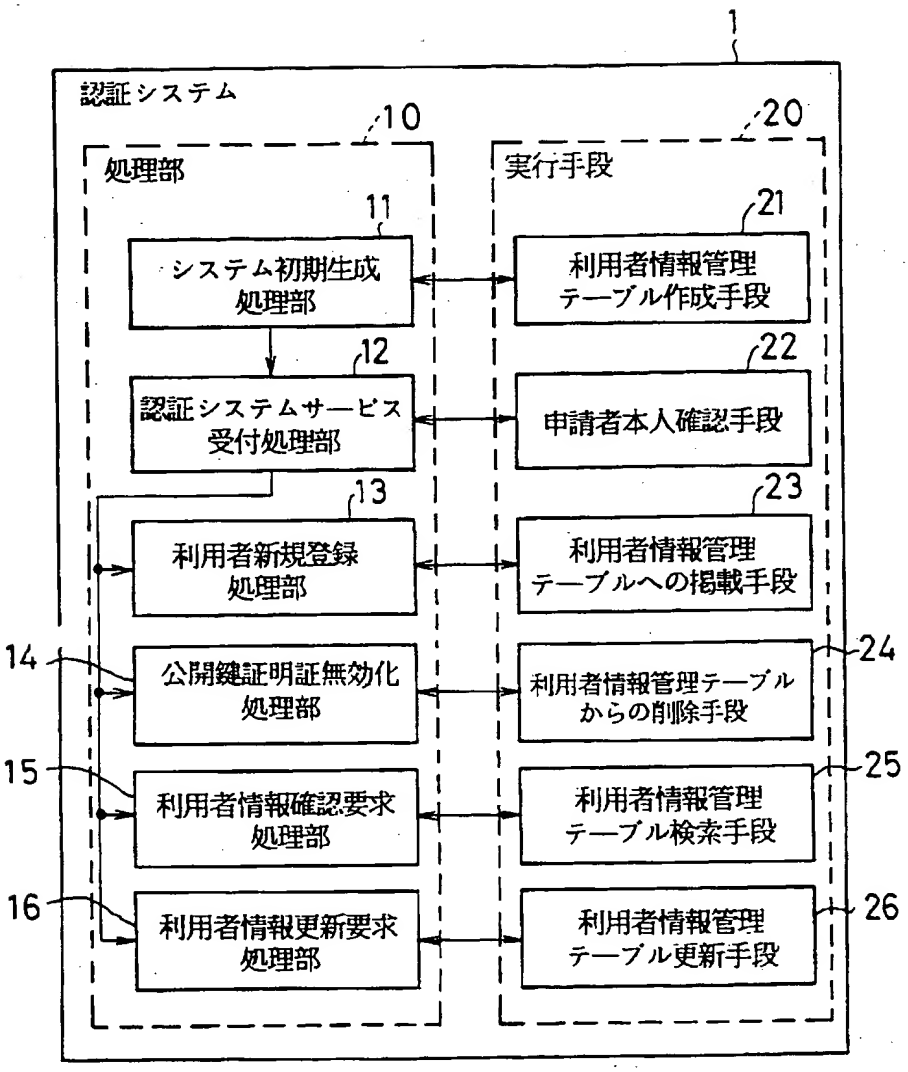
【図６】図１における利用者情報確認要求処理を説明するためのブロック図である。

【図７】図１における利用者情報更新要求処理を説明するためのブロック図である。

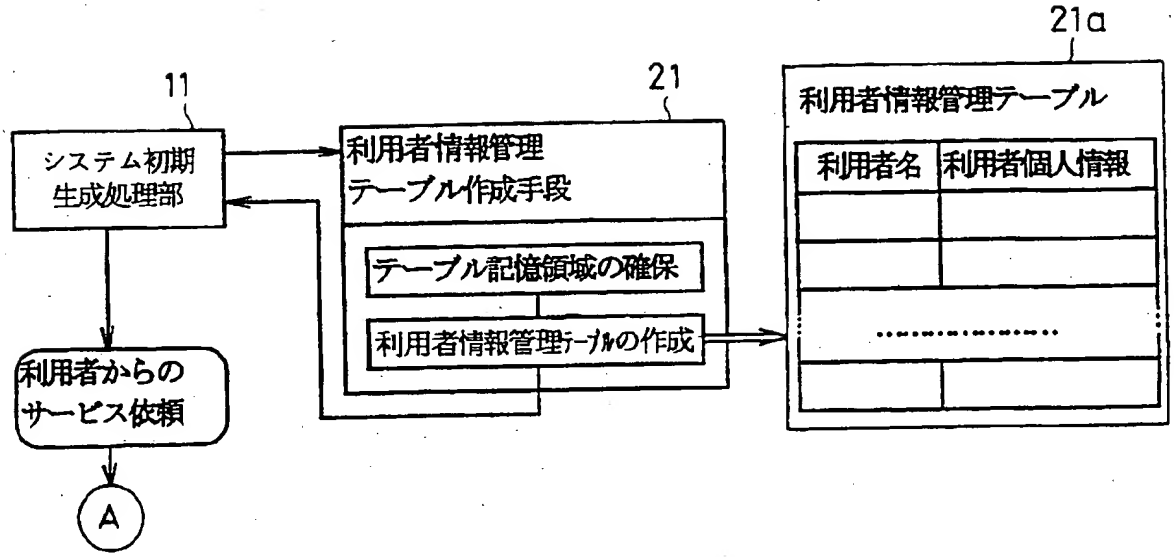
【符号の説明】

１１　システム初期生成処理部
１２　認証システムサービス受付処理部
１３　利用者新規登録処理部
１４　公開鍵証明証無効化処理部
１５　利用者情報確認要求処理部
１６　利用者情報更新要求処理部
２１　利用者情報管理テーブル作成手段
２２　申請者本人確認手段
２３　利用者情報管理テーブルへの掲載手段
２４　利用者情報管理テーブルからの削除手段
２５　利用者情報管理テーブル検索手段
２６　利用者情報管理テーブル更新手段
２１ａ　利用者情報管理テーブル
２２ａ　申請書
２２ｂ　公開鍵証明証管理データベース

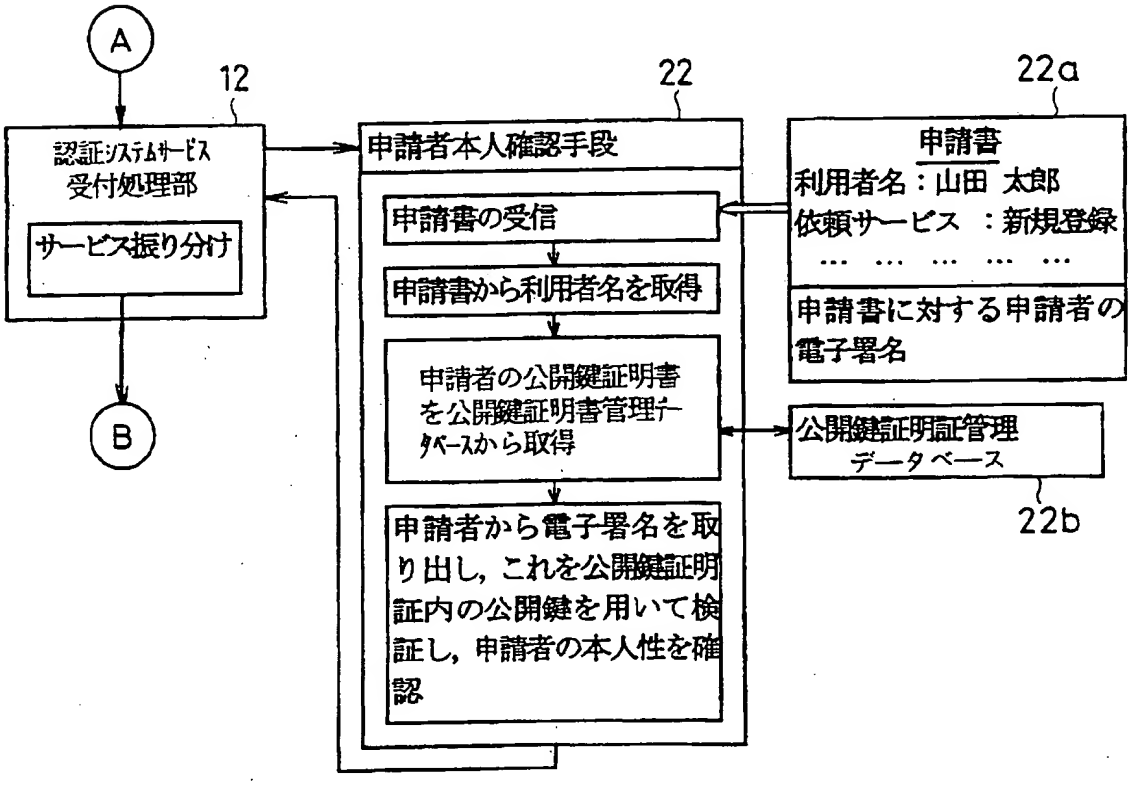
【図1】


1
認証システム
10
処理部
11
システム初期生成処理部
12
認証システムサービス受付処理部
13
利用者新規登録処理部
14
公開鍵証明証無効化処理部
15
利用者情報確認要求処理部
16
利用者情報更新要求処理部
20
実行手段
21
利用者情報管理テーブル作成手段
22
申請者本人確認手段
23
利用者情報管理テーブルへの掲載手段
24
利用者情報管理テーブルからの削除手段
25
利用者情報管理テーブル検索手段
26
利用者情報管理テーブル更新手段

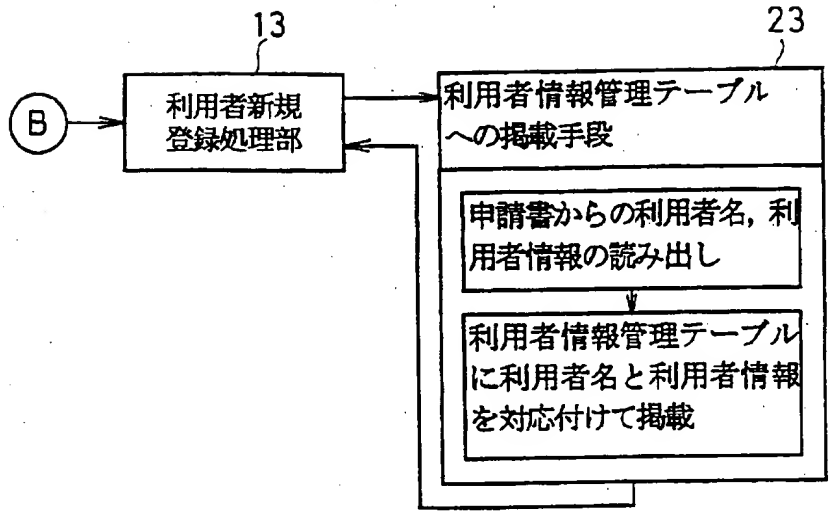
【図2】


21a
11
21
利用者情報管理テーブル
システム初期生成処理部
利用者情報管理テーブル作成手段
利用者名
利用者個人情報
テーブル記憶領域の確保
利用者情報管理テーブルの作成
利用者からのサービス依頼
A

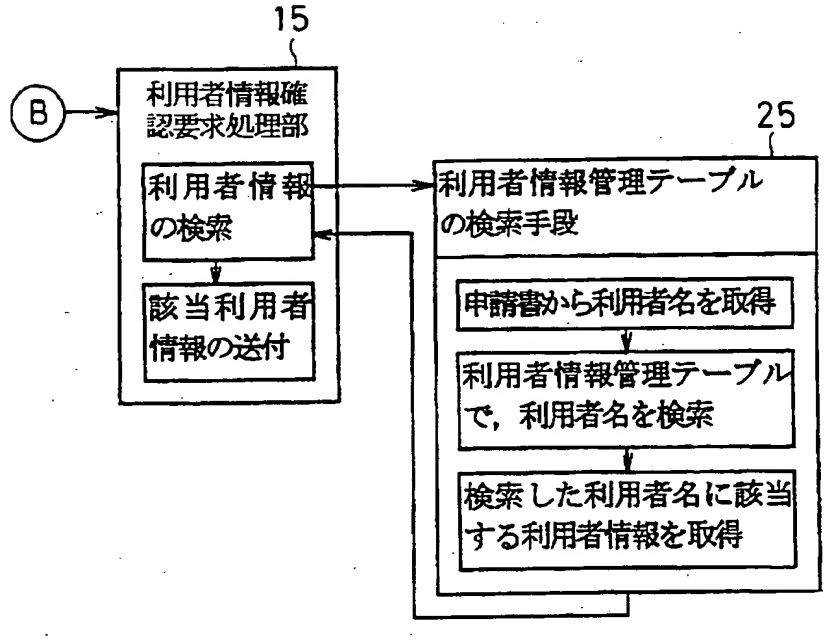
【図3】


A
12
22
22a
認証システムサービス受付処理部
サービス振り分け
申請者本人確認手段
申請書
利用者名：山田 太郎
依頼サービス ：新規登録
申請書の受信
申請書から利用者名を取得
申請書に対する申請者の電子署名
申請者の公開鍵証明書を公開鍵証明書管理データベースから取得
公開鍵証明証管理データベース
22b
申請者から電子署名を取り出し，これを公開鍵証明証内の公開鍵を用いて検証し，申請者の本人性を確認
B

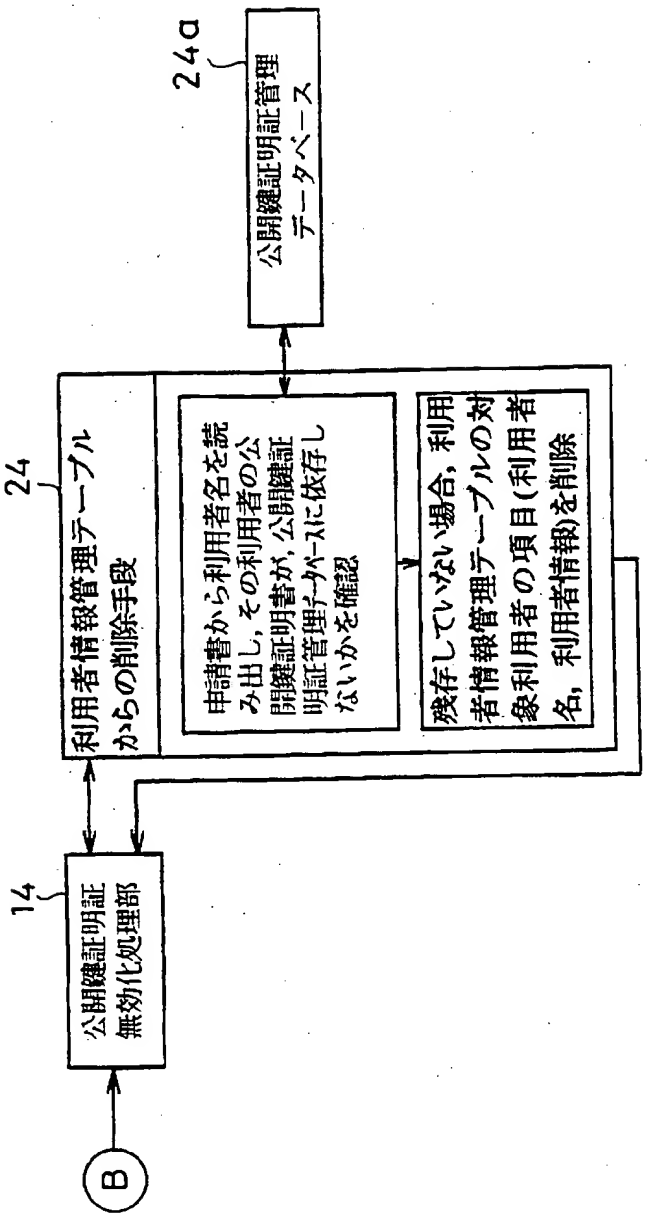
【図4】


13
23
B
利用者新規登録処理部
利用者情報管理テーブルへの掲載手段
申請書からの利用者名，利用者情報の読み出し
利用者情報管理テーブルに利用者名と利用者情報を対応付けて掲載

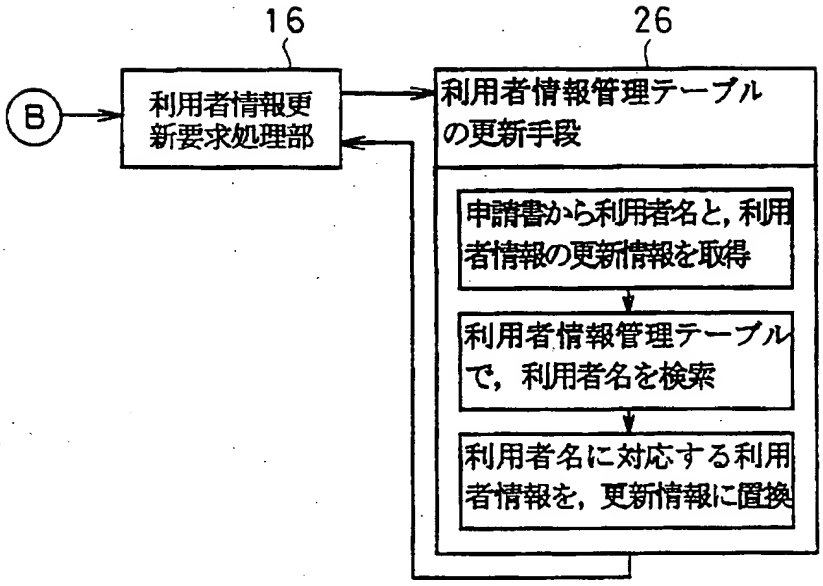
【図6】


15
25
B
利用者情報確認要求処理部
利用者情報の検索
該当利用者情報の送付
利用者情報管理テーブルの検索手段
申請書から利用者名を取得
利用者情報管理テーブルで，利用者名を検索
検索した利用者名に該当する利用者情報を取得

【図5】


24a
公開鍵証明証管理データベース
24
利用者情報管理テーブルからの削除手段
申請書から利用者名を読み出し，その利用者の公開鍵証明書が，公開鍵証明証管理データベースに依存しないかを確認
残存していない場合，利用者情報管理テーブルの対象利用者の項目(利用者名，利用者情報)を削除
14
公開鍵証明証無効化処理部
B

【図7】




---

フロントページの続き

(72)発明者　中原　慎一
神奈川県横浜市中区山下町223番1　エヌ・ティ・ティ・ソフトウェア株式会社内